

FEB 24 2014

CLERK OF SEATTLE COURT
WESTERN DISTRICT OF WASHINGTON DEPUTY

UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

Digital Devices seized from 704 South 209th Street,
Des Moines, WA

Case No.

MD14-66

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Digital devices seized from 704 South 209th Street, Des Moines, WA, currently located at the HSI Seattle computer forensics lab, located at 1000 2nd Ave, Seattle, WA, as described further in Attachment A to attached affidavit.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B to attached affidavit

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 USC 2251	Production of Child Pornography
18 USC 2252	Possession of Child Pornography

The application is based on these facts:
See attached affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

SA Timothy Ensley, HSI

Printed name and title

Sworn to before me and signed in my presence.

Date: Feb 24, 2014

City and state: Seattle, WA



Judge's signature

Brian Tsuchida

Printed name and title

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 0
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 0
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8

SS

7

8

9
0
1
2
3
4
5
6
7
8
9
0
1
2
3
4
5
6

27
28

1 seized (the "DIGITAL MEDIA") by Des Moines, Washington Police Department (the
2 "DMPD") from WILCKEN's residence located at 704 South 209th Street, Des Moines,
3 Washington (the "SUBJECT PREMISES") on March 10, 2010. The DIGITAL MEDIA
4 are more fully described in Attachment A to this Affidavit, and are currently being stored
5 in the secure facilities of the HSI Seattle computer forensics lab, located at 1000 2nd
6 Avenue, Suite 2300, Seattle, Washington 98104.

7 3. The facts set forth in this Affidavit are based on my own personal
8 knowledge; knowledge obtained from other individuals during my participation in this
9 investigation, including other law enforcement officers; interviews of cooperating
10 witnesses; review of documents and records related to this investigation; communications
11 with others who have personal knowledge of the events and circumstances described
12 herein; and information gained through my training and experience.

13 4. Because this Affidavit is submitted for the limited purpose of establishing
14 probable cause in support of the application for a search warrant, it does not set forth
15 each and every fact that I or others have learned during the course of this investigation. I
16 have set forth only the facts that I believe are relevant to the determination of probable
17 cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §
18 2251(a), Production of Child Pornography, 18 U.S.C. § 2252(a)(2), Receipt or
19 Distribution of Child Pornography, and 18 U.S.C. § 2252(a)(4)(B), Possession of Child
20 Pornography, will be found within the DIGITAL MEDIA, described in Attachment B to
21 this Affidavit.

22 II. SUMMARY OF INVESTIGATION

23 5. Homeland Security Investigations (HSI), Seattle and the United States
24 Attorney's Office in Seattle are currently investigating Daniel John WILCKEN) for
25 production of child pornography. As explained in more detail below, based on
26 allegations of a child sex crime, DMPD conducted a state search warrant at WILCKEN's
27 residence in Des Moines on March 10, 2010 and seized digital media and other evidence.
28 A subsequent forensic examination of the seized digital media revealed depictions of

1 WILCKEN's two minor daughters as well as other identified and unidentified minor
2 females, engaged in sexually explicit conduct. Statements made to law enforcement by
3 some of these minor females implicate WILCKEN as the producer of these illegal
4 depictions.

5 6. Based on conduct described in part herein, on December 13, 2013,
6 WILCKEN was convicted by a jury in King County, Washington District Court, of the
7 following criminal violations:

- 8 -Count 1: Child Molestation In The Second Degree
- 9 -Count 2: Attempted Child Molestation In The Second Degree
- 10 -Count 3: Child Molestation In The First Degree
- 11 -Count 4: Attempted Child Molestation In The Second Degree

12 7. On January 22, 2014, WILCKEN was sentenced to 198 months in prison on
13 an indeterminate sentence.

14 III. INVESTIGATION

15 8. In February 2009, the DMPD began an investigation into WILCKEN after
16 allegations of a child sex crime were made by one of WILCKEN's minor daughters'
17 friends, C.S.

18 9. C.S. told DMPD Officers that in 2005, she was approximately 12 years old
19 when she first met WILCKEN's daughters, C.W. and E.W.), who were approximately 13
20 and 12 years old at the time. C.S. told officers that she often visited C.W. and E.W. at
21 their residence located at 704 South 209th, Des Moines, Washington (hereinafter
22 "SUBJECT PREMISES"), for sleepovers and after-school activities.

23 10. C.S., C.W. and E.W. were actively involved in a middle school activity
24 group with numerous other female students centered on a Japanese style cartoon or
25 "Anime." WILCKEN was a parent advisor of the group.

26 11. C.S. stated that in 2005, during a sleepover at the SUBJECT PREMISES,
27 WILCKEN told C.S. he needed photos of a slumber party for a photo shoot project he
28 was doing. C.S. said she was dressed in pajamas and together with E.W. they had a

1 pillow fight while WILCKEN took photos of them. WILCKEN then asked C.S. and
2 E.W. to kiss. C.S. said she initially refused but E.W. pulled her close and kissed her
3 while WILCKEN took photos.

4 12. C.S. stated that in 2006-2007, she became interested in costume design and
5 WILCKEN took photos of her and her juvenile female friends in various dresses,
6 costumes and bathing suits. C.S. said that since 2006-2007 when she was 13 years old
7 and as recently as December of 2009, WILCKEN asked C.S. numerous times if she were
8 ready to take nude photos, claiming he needed the nude photos for a computer animation
9 program he was doing. C.S. said she refused to be photographed naked. C.S. said she
10 was also present when WILCKEN asked her two juvenile female friends if they were
11 ready to be photographed in the nude. C.S. stated that she and the other girls refused.

12 13. C.S. told officers that in 2007, after one of the photo shoots at the
13 SUBJECT PREMISES, she sat down with WILCKEN and C.W. at WILCKEN's
14 computer to review the photos and to transfer the photos onto C.S.'s MySpace page. C.S.
15 stated that while at the computer, she saw photos of C.W. naked. C.S. stated that when
16 she asked what it was, WILCKEN told her "those are the naked photos, do you want to
17 see them?" C.S. said that when she asked WILCKEN if he had naked photos of his
18 daughters, he told her he did and offered to show them to her. C.S. stated that
19 WILCKEN then began opening files on his computer.

20 14. C.S. described to officers seeing at least 30-40 nude photos of C.W. when
21 she was 16 years old, which showed C.W.'s breast and vaginal area. C.S. described
22 observing one explicit photo of C.W., which depicted C.W. sitting down with her legs
23 spread open with a close-up of her vagina.

24 15. When asked by C.S. why he had naked photos of his daughters, WILCKEN
25 explained that it was for an animation program and needed nude photos in order to make
26 a person with the computer program.

27 16. C.S. also reported seeing photos on WILCKEN's computer of E.W. when
28 she was approximately 15 years old dressed in only her bra and underwear. C.S. also

1 reported observing at least ten nude images on WILCKEN's computer of a juvenile
2 female C.S. knew only as "Sierra." "Sierra," has now been identified as C.B., a friend of
3 WILCKEN's daughters.

4 17. C.S. said she did the modeling photo shoots and viewed the nude and
5 clothed photos of C.W., E.W, and C.B. on a computer that was located in the downstairs
6 basement of the SUBJECT PREMISES. C.S. described the computer room as having
7 multiple computers and two large monitors.

8 18. C.S. described the photography room as being across the hall from the
9 computer room and equipped with a white pull down backdrop. C.S. said behind the
10 backdrop is a small closet which had been converted into a sound proof room which is
11 equipped with a microphone. C.S. said she saw nude photos on WILCKEN's computer
12 of C.B. that were photographed in the sound proof room.

13 19. In February 2010, as DMPD continued to investigate the matter, DMPD
14 Detective Paul Young made contact with C.S. with follow-up questions.

15 20. C.S. told officers that she had seen the folder containing various nude
16 photos of C.W. on WILCKEN's home computer a total of three times, the first being in
17 2007 and the last in 2009. C.S. also described seeing images of C.W. lying naked on a
18 bed and in the shower. C.S. stated that the folder containing the nude photos was
19 "hidden" within WILCKEN's computer.

20 21. C.S. then told officers that one of her friends, H.J. had recently admitted to
21 C.S. that she had posed nude for WILCKEN at the SUBJECT PREMISES.

22 22. Detective Young later made contact with H.J. and requested to speak with
23 her about WILCKEN. H.J. agreed to speak with officers.

24 23. H.J. told DMPD officers that she had posed nude for WILCKEN at the
25 SUBJECT PREMISES. H.J. said that she was approximately 12 or 13 years old when
26 she first posed nude for WILCKEN.

27 24. On March 8, 2010, Detective Young presented a search warrant affidavit to
28 King County, WA District Court Judge David Christie seeking permission to search the

1 SUBJECT PREMISES for evidence of child exploitation violations. Judge Christie
2 authorized the search of the SUBJECT PREMISES.

3 25. On March 10, 2010, DMPD officers searched WILCKEN's home and
4 recovered numerous computers, computer hard drives, and other evidence. Some of
5 WILCKEN's digital media were then forensically examined by Washington State Patrol
6 Detective Jason Keays.

7 26. Detective Keays' forensic examination included a review of six hard drives
8 taken from a server located in WILCKEN's production room within the SUBJECT
9 PREMISES. On one hard drive, Detective Keays located over 2000 images of a minor
10 female named "Little Melissa" in various outfits including a French maid outfit. The
11 same hard drive contained approximately 11,500 photos of a girl named "Nicky." These
12 photos show "Nicky" in various outfits, many of which show "Nicky" with her legs
13 spread exposing her panties to the viewer.

14 27. On the same drive, Detective Keays located more than 1,100 images of a
15 female in various stages of undress. Each of these photos included a file name with the
16 initials, "DJW," which are the initials of the defendant's eldest daughter. Many of the
17 photos of WILCKEN's minor daughter focus on her breasts and vagina. On another hard
18 drive, Detective Keays found still other nude photos of WILCKEN's minor daughter in a
19 bathtub and shower scene. On yet another hard drive, Detective Keays found over 8000
20 images of young girls in Christmas outfits. Some of the photos are taken from an angle,
21 which show the girls are not wearing underwear. Two images show the girls posing with
22 their breasts exposed. These photos were found in a folder labeled "...Internet
23 Websites\byjoveentertainment\...\ DELETEME-kelly-girls..." WILCKEN is listed as the
24 Chief Executive Officer of "By Jove Entertainment" on the company's website,
25 "byjove.com."

26 28. I have obtained a DVD from DMPD, which contains the WSP computer
27 forensic examination reports, among other reports, in this case. The reports include
28 image and video files of suspected child pornography found on some of WILCKEN's

1 digital media devices, some of which depict WILCKEN's minor daughters engaged in
2 sexually explicit activity. I have reviewed these files, and based on my knowledge,
3 training and experience in investigating Internet crimes against children, I believe many
4 of these depictions meet the federal definition of child pornography.

5 29. I have described one of these images below:

6 File Name: djw070506-033.jpg - This color image depicts a white female,
7 identified as WILCKEN's minor daughter, C.W., completely nude, sitting on what
8 appears to be a white floor. C.W. is facing the camera while leaning back with both
9 elbows on the floor propping her upper body up. C.W.'s legs are spread open fully
10 exposing her genital area. C.W. can be seen from the top of her head to just above her
11 knees. C.W. shows some breast development and some pubic hair growth. The file
12 name contains the initials "djw," which are WILCKEN's initials, as well as the date
13 "070506." On July, 5, 2006, C.W. was 14 years of age.

14 30. The investigation by DMPD and HSI Seattle, through witness and victim
15 statements and a preliminary review of a portion of the DIGITAL MEDIA, has revealed
16 that there may be additional child victims of WILCKEN's alleged production of child
17 pornography that have yet to be identified and located on the DIGITAL MEDIA. The
18 investigation has also revealed that there may be additional producers of child
19 pornography involved in this case, who may have directly assisted WILCKEN in his
20 alleged criminal activity. Specifically, Detective Keays did not forensically review all of
21 the DIGITAL MEDIA seized from the SUBJECT RESIDENCE, which comprised 18
22 Desktop Computer Towers and 33 hard drives, and other DIGIAL MEDIA set forth in
23 full in Attachment A. A more detailed and coordinated review of the DIGITAL MEDIA
24 in this case may allow law enforcement to identify these child victims, as well as identify
25 additional producers of child pornography.

26 31. On February 4, 2014, HSI Seattle took custody of the DIGITAL MEDIA
27 seized by DMPD during the state search warrant executed SUBJECT PREMISES on
28 March 10, 2010, as well as DMPD's reports and investigative findings in this case. The

1 seized property is currently being stored in a secure computer forensics lab within the
2 HSI Seattle offices, located at 1000 2nd Avenue, Suite 2300, Seattle, Washington 98104.

3 **IV. DEFINITIONS AND TECHNICAL TERMS**

4 32. Set forth below are some definitions of technical terms, most of which are
5 used throughout this Affidavit pertaining to the Internet and computers generally.

6 a. Computers, Digital Media and digital devices: As used in this
7 Affidavit, the terms "computer" and "digital device," along with the terms "electronic
8 storage media," "digital storage media," and "data storage device," refer to those items
9 capable of storing, creating, transmitting, displaying, or encoding electronic or digital
10 data, including computers, hard drives, thumb drives, flash drives, memory cards, media
11 cards, smart cards, PC cards, digital cameras and digital camera memory cards, electronic
12 notebooks and tablets, smart phones and personal digital assistants, printers, scanners,
13 and other similar items.

14 b. Hash Value: "Hashing" refers to the process of using a
15 mathematical function, often called an algorithm, to generate a numerical identifier for
16 data. This numerical identifier is called a "hash value." A hash value can be thought of
17 as a "digital fingerprint" for data. If the data is changed, even very slightly (like through
18 the addition or deletion of a comma or a period in a text file), the hash value for that data
19 would change. Therefore, if a file such as a digital photo is a hash value match to a
20 known file, it means that the digital photo is an exact copy of the known file.

21 **V. TECHNICAL BACKGROUND**

22 33. As part of my training, I have become familiar with the Internet (also
23 commonly known as the World Wide Web), a global network of computers and other
24 electronic devices that communicate with each other using various means, including
25 standard telephone lines, high speed telecommunications links (e.g., copper and fiber
26 optic cable), and wireless transmissions, including satellite. Due to the structure of the
27 Internet, connections between computers on the Internet routinely cross state and
28 international borders, even when the computers communicating with each other are in the

1 same state. Individuals and entities use the Internet to gain access to a wide variety of
2 information; to send information to, and receive information from, other individuals; to
3 conduct commercial transactions; and to communicate via email.

4 34. As set forth above, I seek permission to search the DIGITAL MEDIA listed
5 in Attachment A to this Affidavit for evidence, fruits, and instrumentalities of the above-
6 referenced crimes. It has been my experience that individuals involved in child
7 pornography often prefer to store images of child pornography in electronic form. The
8 ability to store images of child pornography in electronic form makes digital devices an
9 ideal repository for child pornography. The images can be easily sent or received from
10 other digital media device users over the Internet. Further, both individual files of child
11 pornography and any storage media that contain them can be mislabeled or hidden to
12 evade detection. In my training and experience, individuals who view child pornography
13 typically maintain their collections for many years and keep and collect items containing
14 child pornography over long periods of time; in fact, they rarely, if ever, dispose of their
15 sexually explicit materials. As a result, one form in which these items may be found is as
16 electronic evidence stored on a digital device.

17 a. Based upon my knowledge, training, and experience in child
18 exploitation and child pornography investigations, and the experience and training of
19 other law enforcement officers with whom I have had discussions, I know that computers
20 and computer technology have revolutionized the way in which child pornography is
21 collected, distributed, produced and utilized, and the way in which those who seek out
22 child pornography are able to obtain this material. Computers serve four basic functions
23 in connection with child pornography: production, communication, distribution, and
24 storage. More specifically, the development of computers has changed the methods used
25 by those who seek to obtain access to child pornography as described in subparagraphs
26 (b) through (e) below.

27 b. Producers of child pornography can now produce both still and
28 moving images directly from a common video or digital camera. The camera is attached,

1 using a device such as a cable, or digital images are often uploaded from the camera's
2 memory card, directly to the computer. Images can then be stored, manipulated,
3 transferred, or printed directly from the computer. Images can be edited in ways similar
4 to how a photograph may be altered. Images can be lightened, darkened, cropped, or
5 otherwise manipulated. The producers of child pornography can also use a device known
6 as a scanner to transfer photographs into a computer readable format. As a result of this
7 technology, it is relatively inexpensive and technically easy to produce, store, and
8 distribute child pornography. In addition, there is an added benefit to the pornographer in
9 that this method of production does not leave as large a trail for law enforcement to
10 follow.

11 c. The Internet allows any computer to connect to another computer.
12 Peer-to-Peer ("P2P") file sharing is one way in which Internet users connect to each other
13 to form a digital network, which allows for the sharing of digital files between users. P2P
14 networks are one of the fastest growing avenues by which child pornography collectors
15 and traders acquire and share their collections of child pornography. A user obtains
16 publicly available P2P software, which can be downloaded from the Internet, and installs
17 it on his computer. The P2P user then selects files from his computer to share with others
18 on the P2P network, and makes them available for download by other P2P users. Each
19 time the user runs the P2P file-sharing program, his computer establishes a connection
20 with other computers on the file-sharing network. The user can then search the network
21 for files of interest, including child pornography, by conducting a keyword search for
22 files using search terms such as "PTHC," a recognized abbreviation for "pre-teen hard
23 core."

24 d. The Internet allows users, while still maintaining anonymity, to
25 easily locate (i) other individuals with similar interests in child pornography and (ii)
26 websites that offer images of child pornography. Through the use of computers and the
27 Internet, distributors of child pornography are also able to maintain their anonymity by
28 using membership- and/or subscription-based websites to conduct business. Those who

1 seek to obtain images or videos of child pornography can use standard Internet
2 connections, such as those provided by businesses, universities, and government
3 agencies, to communicate with each other and to distribute child pornography. These
4 communication links allow contacts around the world as easily as calling next door.
5 Additionally, these communications can be quick, relatively secure, and as anonymous as
6 desired. All of these advantages, which promote anonymity for both the distributor and
7 recipient, are well known and are the foundation of transactions involving those who
8 wish to gain access to child pornography over the Internet. Sometimes the only way to
9 identify both parties and verify the transportation of child pornography over the Internet
10 is to examine the recipient's computer, including the Internet history and cache to look for
11 "footprints" of the websites and images accessed by the recipient.

12 e. The computer's capability to store images in digital form makes it an
13 ideal repository for child pornography. A single floppy disk can store dozens of images
14 and hundreds of pages of text. The size of the electronic storage media (commonly
15 referred to as a "hard drive") used in home computers has grown tremendously within the
16 last several years. Hard drives with the capacity of 500 gigabytes or 1 terabyte are not
17 uncommon. These drives can store thousands of images at very high resolution.
18 Magnetic storage located in host computers adds another dimension to the equation. It is
19 possible to use a video camera to capture an image, process that image in a computer
20 with a video capture board, and save that image to storage in another country. Once this
21 is done, there is no readily apparent evidence at the "scene of the crime." Only with
22 careful laboratory examination of electronic storage devices is it possible to recreate the
23 evidence trail.

24 35. Based upon my knowledge, experience, and training in child pornography
25 investigations, and the training and experience of other law enforcement officers with
26 whom I have had discussions, I know that there are certain characteristics common to
27 individuals involved in child pornography:
28

1 a. Those who receive and attempt to receive child pornography may
2 receive sexual gratification, stimulation, and satisfaction from contact with children; or
3 from fantasies they may have viewing children engaged in sexual activity or in sexually
4 suggestive poses, such as in person, in photographs, or other visual media; or from
5 literature describing such activity.

6 b. Those who receive and attempt to receive child pornography may
7 collect sexually explicit or suggestive materials, in a variety of media, including
8 photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or
9 other visual media. Such individuals often times use these materials for their own sexual
10 arousal and gratification. Further, they may use these materials to lower the inhibitions
11 of children they are attempting to seduce, to arouse the selected child partner, or to
12 demonstrate the desired sexual acts.

13 c. Likewise, those who receive and attempt to receive child
14 pornography often maintain their collections that are in a digital or electronic format in a
15 safe, secure and private environment, such as a computer and surrounding area. These
16 collections are often maintained for several years and are kept close by, usually at the
17 individual's residence, to enable the collector to view the collection, which is valued
18 highly.

19 d. Those who receive and attempt to receive child pornography also
20 may correspond with and/or meet others to share information and materials; rarely
21 destroy correspondence from other child pornography distributors/collectors; conceal
22 such correspondence as they do their sexually explicit material; and often maintain lists
23 of names, addresses, and telephone numbers of individuals with whom they have been in
24 contact and who share the same interests in child pornography.

25 e. Those who receive and attempt to receive child pornography prefer
26 not to be without their child pornography for any prolonged time period. This behavior
27 has been documented by law enforcement officers involved in the investigation of child
28 pornography throughout the world.

1 36. Based on my training and experience, and that of computer forensic agents
2 that I work and collaborate with on a daily basis, who collectively have over seven years
3 of specialized training and experience in searching for electronic evidence, I know that
4 every type and kind of information, data, record, sound or image can exist and be present
5 as electronically stored information on any of a variety of computers, computer systems,
6 digital devices, and other electronic storage media. I also know that electronic evidence
7 can be moved easily from one digital device to another. As a result, I believe that
8 electronic evidence may be stored on any piece of the DIGITAL MEDIA seized from
9 IRVING, as is further described in Attachment A to this Affidavit.

10 a. With respect to the digital camera and video camera, these digital
11 devices are capable of creating data, inasmuch as they can be used to take still images
12 and record videos, and of storing data. Digital cameras and video cameras contain a
13 small amount of internal memory, used both to support their operating systems and to
14 store a small amount of device-generated data, i.e., images and videos.

15 b. Memory cards are capable of storing data from multiple sources. In
16 that sense, they function much like thumb drives. I am aware that it is possible to store
17 images and videos on memory cards, regardless of whether those images and videos were
18 created with the digital device in which the particular memory card is found. Image and
19 video files from a computer can be transferred onto a memory card when it is directly
20 inserted into a computer. Likewise, if a digital camera or video camera is connected to a
21 computer through a USB cable, image and video files can be transferred back and forth
22 from the memory card in the camera to the computer.

23 37. Based on my training and experience, and my consultation with computer
24 forensic agents who are familiar with searches of computers, I know that in some cases
25 the items set forth in Attachment B may take the form of files, documents, and other data
26 that is user-generated and found on a digital device. In other cases, these items may take
27 the form of other types of data – including in some cases data generated automatically by
28 the devices themselves.

1 38. Based on my training and experience, information I have obtained from the
2 KKSO, and my consultation with computer forensic agents who are familiar with
3 searches of computers, I believe that there is probable cause to believe that evidence,
4 fruits, and instrumentalities relating to child pornography will be present on the
5 DIGITAL MEDIA described in Attachment A for a number of reasons, including but not
6 limited to the following:

7 a. Once created, electronically stored information ("ESI") can be stored
8 for years in very little space and at little or no cost. A great deal of ESI is created, and
9 stored, moreover, even without a conscious act on the part of the device operator. For
10 example, files that have been viewed via the Internet are sometimes automatically
11 downloaded into a temporary Internet directory or "cache," without the knowledge of the
12 device user. The browser often maintains a fixed amount of hard drive space devoted to
13 these files, and the files are only overwritten as they are replaced with more recently
14 viewed Internet pages or if a user takes steps to delete them. This ESI may include
15 relevant and significant evidence regarding criminal activities, but also, and just as
16 important, may include evidence of the identity of the device user, and when and how the
17 device was used. Most often, some affirmative action is necessary to delete ESI. And
18 even when such action has been deliberately taken, ESI can often be recovered, months
19 or even years later, using forensic tools.

20 b. Wholly apart from data created directly (or indirectly) by user-
21 generated files, digital devices – in particular, a computer's internal hard drive – contain
22 electronic evidence of how a digital device has been used, what it has been used for, and
23 who has used it. This evidence can take the form of operating system configurations,
24 artifacts from operating systems or application operations, file system data structures, and
25 virtual memory "swap" or paging files. Computer users typically do not erase or delete
26 this evidence, because special software is typically required for that task. However, it is
27 technically possible for a user to use such software to delete this type of information -
28

1 and, the use of such special software may itself result in ESI that is relevant to the
2 criminal investigation.

3 VI. SEIZURE OF DIGITAL DEVICES

4 39. On March 8, 2010, Detective Young obtained a search warrant issued from
5 the King County, Washington District Court. On March 10, 2010, DMPD led the
6 execution of the search warrant at the SUBJECT PREMISES. A number of digital
7 devices were seized pursuant to that warrant. The DIGITAL MEDIA this warrant
8 application seeks permission to search are currently located in the secure computer
9 forensics lab of HSI Seattle, 1000 2nd Avenue, Suite 2300, Seattle, Washington 98104.

10 VII. SEARCH OF THE DIGITAL MEDIA

11 40. As set forth above, I seek permission to search the DIGITAL MEDIA
12 described in Attachment A for the things described in Attachment B, that is, evidence,
13 fruits, and instrumentalities of the above-referenced crimes, in whatever form they may
14 be found. In accordance with the information in this Affidavit, law enforcement
15 personnel, to include the case agent, will execute the search of the DIGITAL MEDIA
16 seized pursuant to this warrant as follows:

17 a. In order to examine the ESI in a forensically sound manner, law
18 enforcement personnel with appropriate expertise will produce a complete forensic
19 image, if possible, of the DIGITAL MEDIA listed in Attachment A to this Affidavit. In
20 addition, appropriately trained personnel may search for and attempt to recover deleted,
21 hidden, or encrypted data to determine whether the data fall within the list of items in
22 Attachment B. In order to search fully for these items, law enforcement personnel may
23 then examine all of the data contained in the forensic image/s and/or on the DIGITAL
24 MEDIA to view their precise contents and determine whether the data fall within the list
25 of items in Attachment B.

26 b. The search techniques that will be used will be only those
27 methodologies, techniques and protocols as may reasonably be expected to find, identify,
28 segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to

1 this Affidavit. In this particular case, the government anticipates the use of a "hash
2 value" library to exclude normal operating system files that do not need to be searched,
3 which will further facilitate the search for items described in Attachment B. Further, the
4 government anticipates the use of hash sets and known file filters to assist the digital
5 forensics examiners/agents in identifying known and or suspected child pornography
6 image files. Use of these tools will allow for the identification of evidentiary files but
7 also assist in the filtering of normal system files that would have no bearing on the case.

8 c. If, after conducting its examination, law enforcement personnel
9 determine that any of the DIGITAL MEDIA listed in Attachment A are an
10 instrumentality of the criminal offenses referenced above, the government may retain that
11 device during the pendency of the case as necessary to, among other things, preserve the
12 instrumentality evidence for trial, ensure the chain of custody, and litigate the issue of
13 forfeiture. If law enforcement personnel determine that a device was not an
14 instrumentality of the criminal offenses referenced above, it shall be returned to the
15 person/entity from whom it was seized within 90 days of the issuance of the warrant,
16 unless the government seeks and obtains authorization from the court for its retention.

17 d. Unless the government seeks an additional order of authorization
18 from any Magistrate Judge in the District, the government will return any digital device
19 that has been forensically copied, that is not an instrumentality of the crime, and that may
20 be lawfully possessed by the person/entity from whom it was seized, to the person/entity
21 from whom it was seized within 90 days of seizure.

22 VIII. INSTRUMENTALITIES

23 41. Based on the information in this Affidavit, I also believe that the DIGITAL
24 MEDIA listed in Attachment A are instrumentalities of crime and constitute the means by
25 which violations of 18 U.S.C. § 2251(a), Production of Child Pornography, 18 U.S.C. §
26 2252(a)(2), Receipt or Distribution of Child Pornography, and 18 U.S.C. § 2252(a)(4)(B),
27 Possession of Child Pornography, have been committed. Therefore, I believe that in
28 addition to seizing the DIGITAL MEDIA listed in Attachment A to conduct a search of

1 their contents as set forth herein, there is probable cause to seize those DIGITAL MEDIA
2 as instrumentalities of criminal activity.

3 **IX. CONCLUSION**

4 42. Based on the foregoing, I believe there is probable cause that evidence,
5 fruits, and instrumentalities of violations of 18 U.S.C. § 2251(a), Production of Child
6 Pornography, 18 U.S.C. § 2252(a)(2), Receipt or Distribution of Child Pornography, and
7 18 U.S.C. § 2252(a)(4)(B), Possession of Child Pornography, are located on the
8 DIGITAL MEDIA, as more fully described in Attachment A to this Affidavit. I therefore
9 request that the court issue a warrant authorizing a search of these DIGITAL MEDIA for
10 the items more fully described in Attachment B hereto and incorporated herein by
11 reference.

12
13 

14 TIMOTHY ENSLEY, Affiant
15 Special Agent
16 U.S. Department of Homeland Security
17 Homeland Security Investigations

18
19 SUBSCRIBED and SWORN to before me this 24 day of February, 2014.

20
21 

22 BRIAN A. TSUCHIDA
23 United States Magistrate Judge
24
25
26
27
28

**ATTACHMENT A
PREVIOUSLY SEIZED DIGITAL MEDIA**

The items listed below were previously seized by the DMPD from DANIEL JOHN WILCKEN's residence, located at 22613 SE 4th Street, Sammamish, WA 98074, and are currently located in the secure evidence room of the HSI Seattle, 1000 2nd Avenue, Suite 2300, Seattle, Washington 98104:

- a. (18)-Desktop Computer Towers
- b. (1)-Laptop
- c. (33)-Hard Drives
- d. (1)-Thumb Drive
- e. (246)-CD/DVD
- f. (2)-Cameras
- g. (1)-Camcorder
- h. (1)-Media Card
- i. (1)-8MM Video Camera
- j. (13)-Film Rolls
- k. (164)-VHS Tapes
- l. (62)-Floppy Diskettes
- m. (71)-Video/Audio Cassette Tapes
- n. (15)-DVD Micro Discs
- o. (1)-Miscellaneous Documents/Papers

ATTACHMENT B
ITEMS TO BE SEARCHED FOR

On the DIGITAL MEDIA listed in Attachment A, the following records, documents, files, or materials that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 2251(a), Production of Child Pornography, 18 U.S.C. § 2252(a)(2), Receipt or Distribution of Child Pornography, and 18 U.S.C. § 2252(a)(4)(B), Possession of Child Pornography:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct, in any format or media;

2. E-mail, and other correspondence identifying persons transmitting child pornography, or containing communications with other individuals regarding the sexual abuse of minors or the production of visual depictions of minor(s) engaged in sexually explicit conduct, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer;

3. All electronically-stored invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;

4. Any and all electronically-stored address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography;

5. Any and all electronically-stored address books, names, lists of names, telephone numbers, and addresses of minors;

6. Any and all electronically-stored communications, chats, blogs, and any other records reflecting personal contact or other activities with minors, including non-pornographic visual depictions of minors;

7. Digital evidence of who used, owned or controlled any seized digital device(s) at the time the things described in this warrant were created, edited, or deleted,

1 such as logs, registry entries, saved user names and passwords, documents, and browsing
2 history;

3 8. Evidence of malware that would allow others to control any seized digital
4 device(s) such as viruses, Trojan horses, and other forms of malicious software, as well
5 as evidence of the presence or absence of security software designed to detect malware;
6 as well as evidence of the lack of such malware;

7 9. Evidence of the attachment to the digital device(s) of other storage devices
8 or similar containers for electronic evidence;

9 10. Evidence of counter-forensic programs (and associated data) that are
10 designed to eliminate data from a digital device;

11 11. Evidence of times the digital device(s) was used, and;

12 12. Any other ESI from the digital device(s) necessary to understand how the
13 digital device was used, the purpose of its use, who used it, and when.